

DORA-Dokumentationsanforderungen – Strukturierte Vollständige Checkliste

Diese umfassende Checkliste enthält alle Dokumentationsanforderungen gemäß der EU-Verordnung DORA (Digital Operational Resilience Act). Die Inhalte sind nach Kapiteln und Artikeln strukturiert. Jeder Artikel ist in die Kategorien Strategien, Leit-/Richtlinien und Weitere Dokumentationsanforderungen unterteilt.

Kapitel II – IKT-Risikomanagement

Artikel 6 DORA – IKT-Risikomanagementrahmen

Strategien

- Geschäftsstrategie (Art. 6 Abs. 8 lit. a DORA) diese enthält
 - DOR-Strategie (Digital Operational Resilience Strategy) (Art. 6 Abs. 8 i.V.m. Art. 5 und Abs. 2 lit. d DORA)

Leit- / Richtlinien

- - Richtlinie für das IKT-Risikomanagement
- - Informationssicherheitsleitlinie

Weitere Dokumentationsanforderungen

- - Bericht über die Überprüfung des IKT-Risikomanagementrahmens

Artikel 7 DORA – Schutzmaßnahmen

Leit- / Richtlinien

- - Richtlinie für kryptografische Kontrollen
- - Richtlinie zur Nutzung von Verschlüsselung

Weitere Dokumentationsanforderungen

- - Register aller Zertifikate und Zertifikatspeicher für kritische IKT-Assets

Artikel 8 DORA – Identifizierung

Leit- / Richtlinien

- - Richtlinie für das Management der IKT-Vorgänge (Betrieb)

Weitere Dokumentationsanforderungen

- - Inventar aller IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten
- - Inventar aller kritischen Informations- und IKT-Assets
- - Inventar aller Prozesse, die von IKT-Drittdienstleistern abhängen

Artikel 9 DORA – Schutz und Prävention

Leit- / Richtlinien

- - Richtlinie für Datensicherung (Backup)
- - Richtlinie für Patch- und Update-Management
- - Richtlinie für Management von IKT-Assets

Weitere Dokumentationsanforderungen

- - Verfahren für Backup und Wiederherstellung
- - Verfahren für Schwachstellenmanagement

Artikel 10 DORA – Erkennung

Leit- / Richtlinien

- - Richtlinie für Netzwerksicherheit

Weitere Dokumentationsanforderungen

- - Mechanismen zur Erkennung anomaler Aktivitäten
- - Verfahren für Logging und Überwachung

Artikel 11 DORA – Reaktion und Wiederherstellung

Leit- / Richtlinien

- - IKT-Geschäftsfortführungsleitlinie (inkl. BIA)
- - IKT-Reaktions- und Wiederherstellungspläne

Weitere Dokumentationsanforderungen

- - Aufzeichnungen über Tätigkeiten während der Aktivierung der IKT-GFP

Artikel 12 DORA – Backup und Wiederherstellungsmaßnahmen

Leit- / Richtlinien

- - Richtlinie und Verfahren zum Backup

Weitere Dokumentationsanforderungen

- - Dokumentation der Wiederherstellungsmaßnahmen

Artikel 13 DORA – Lernprozesse und Weiterentwicklung

Leit- / Richtlinien

- - Richtlinie für Schulungen zur digitalen operationellen Resilienz

Weitere Dokumentationsanforderungen

- - Programme zur Sensibilisierung für IKT-Sicherheit

Artikel 14 DORA – Kommunikation

Strategien

- - Kommunikationsstrategie für IKT-bezogene Vorfälle

Leit- / Richtlinien

- - Kommunikationsleitlinien für Mitarbeiter

Weitere Dokumentationsanforderungen

- - Kommunikationspläne und Protokolle im Krisenfall

Artikel 15 DORA – IKT-Projektmanagement

Leit- / Richtlinien

- - Richtlinie für das IKT-Projektmanagement (inkl. Projektrisikobewertung)

Artikel 16 DORA – Beschaffung, Entwicklung und Wartung von IKT-Systemen

Leit- / Richtlinien

- - Richtlinie für Beschaffung, Entwicklung und Wartung von IKT-Systemen

Weitere Dokumentationsanforderungen

- - Verfahren für die sichere Softwareentwicklung

Kapitel III – Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle

Artikel 17 DORA – Behandlung IKT-bezogener Vorfälle

Leit- / Richtlinien

- - Richtlinie für Behandlung IKT-bezogener Vorfälle

Weitere Dokumentationsanforderungen

- - Dokumentation IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen

Artikel 18 DORA – Physische Sicherheit

Leit- / Richtlinien

- - Richtlinie für physische Sicherheit und Umweltereignisse

Artikel 19 DORA – Personalpolitik

Leit- / Richtlinien

- - Richtlinie für Personalpolitik

Artikel 20 DORA – Identitätsmanagement

Leit- / Richtlinien

- - Richtlinie für Identitätsmanagement

Weitere Dokumentationsanforderungen

- - Verfahren für das Identitätsmanagement

Artikel 21 DORA – Zugangs- und Zugriffskontrollen

Leit- / Richtlinien

- - Richtlinie im Rahmen der Kontrolle von Zugangs- und Zugriffsrechten

Weitere Dokumentationsanforderungen

- - Verfahren für Zugangs- und Zugriffsrechte

Artikel 22–23 DORA – Klassifizierung und Berichterstattung von Vorfällen

Leit- / Richtlinien

- - Richtlinie für Klassifizierung IKT-bezogener Vorfälle

Weitere Dokumentationsanforderungen

- - Bericht über gemeldete Vorfälle gemäß RTS CTIR / ITS TIR

Kapitel IV – Testen der digitalen operationalen Resilienz

Artikel 24 DORA – Testverfahren

Leit- / Richtlinien

- - Leitlinien zur Priorisierung und Behebung von Testergebnissen

Weitere Dokumentationsanforderungen

- - Validierungsmethoden
- - Dokumentation der Testergebnisse

Artikel 25 DORA – Resilienztests

Leit- / Richtlinien

- - Programm für die Tests der digitalen operationalen Resilienz

Weitere Dokumentationsanforderungen

- - Dokumentation der Tests der IKT-GFP

Kapitel V – Management von IKT-Drittparteienrisiken

Artikel 28 DORA – Schlüsselprinzipien des Drittparteienmanagements

Strategien

- - Strategie für IKT-Drittparteienrisiko

Leit- / Richtlinien

- - Leitlinie für Nutzung von IKT-Dienstleistungen
- - Leitlinie für Nutzung von kritischen IKT-Diensten

Weitere Dokumentationsanforderungen

- - Informationsregister
- - Ausstiegspläne für Drittparteien

Artikel 29–30 DORA – Aufsicht und Informationspflichten

Leit- / Richtlinien

- - Richtlinie zur Aufrechterhaltung der Compliance mit DORA durch Drittparteien

Weitere Dokumentationsanforderungen

- - Dokumentation über Melde- und Kontrollpflichten gegenüber Aufsichtsbehörden